Claims

What is claimed is:

1. A method for assessing and/or managing risks for an organization, comprising the steps of:

(a) inventorying a plurality of assets of the organization, wherein each asset is defined to be one of an electronic asset type and a location asset type, and wherein the electronic asset type includes computers and networking equipment therefor and the location asset type includes physical locations where the electronic asset types are placed;

(b) identifying at least one criterion defining a security objective of the organization;

(c) identifying one or more inventoried assets that relate to the identified criterion;

(d) formulating one or more metric equations for each identified criterion, each metric equation being defined, in part, by the one or more identified assets, wherein each metric equation yields an outcome value when one or more measurements are made relating to the identified assets; and

(e) assessing the risk to the organization based on the measured values of the one or more metric equations.

2. The method of claim 1, wherein the step (a) comprises the step of:

identifying the plurality of assets and storing the identified assets into a database.

3. The method of claim 2, wherein the step of identifying the plurality of assets comprises at least one of:

electronically scanning the plurality of assets;

interviewing members of the organization to identify the plurality of assets; and manually identifying the plurality of assets.

4. The method of claim 1, wherein the plurality of assets are defined to be one of a user type, a user population type, a data type and a network type in addition to the electronic type and the location type, wherein the user type relates to an individual user and the user population type relates to a group of users.

5. The method of claim 4, further comprising the step of:

establishing at least one relationship between the plurality of assets.

6. The method of claim 5, wherein the step of establishing the at least one relationship further comprises the step of:

linking a first asset define to be in one asset type with a second asset defined to be in another asset type.

7. The method of claim 5, wherein the step of establishing the at least one relationship further comprises the step of:

linking a first asset define to be in one asset type with a second asset defined to be in the same asset type.

8. The method of claim 5, wherein the step (c) further comprises the step of:

identifying one or more inventoried assets that relate to the identified criterion based on the at least one established relationship between the plurality of assets.

9. A system for assessing and/or managing risks for an organization, comprising:

(a) means for identifying and storing a plurality of assets of the organization, wherein each asset is defined to be one of an electronic asset type and a location asset type, and wherein the electronic asset type includes computers and networking equipment therefor and the location asset type includes physical locations where the electronic asset types are placed;

(b) means for identifying a plurality of criteria, each criterion defining a security objective of the organization;

(c) means for identifying a plurality of inventoried assets that relate to each identified criterion; and

(d) means for formulating one or more metric equations for each identified criterion, each metric equation being defined, in part, by the one or more identified assets, wherein each metric equation yields an outcome value when one or more measurements are made relating to the identified assets, thereby allowing a user to assess the risk to the organization based on the measured values of the one or more metric equations.

10. The system of claim 9, wherein the means (a) comprises:

means for identifying the plurality of assets and storing the identified assets into a database.

11. The system of claim 10, wherein the means for identifying the plurality of assets comprises at least one of:

means for electronically scanning the plurality of assets;

means for interviewing members of the organization to identify the plurality of assets; and

means for manually identifying the plurality of assets.

12. The system of claim 9, wherein the plurality of assets are defined to be one of a user type, a user population type, a data type and a network type in addition to the electronic type and the location type, wherein the user type relates to an individual user and the user population type relates to a group of users.

13. The system of claim 12, further comprising:

means for establishing at least one relationship between the plurality of assets.

14. The system of claim 13, wherein the means for establishing the at least one relationship further comprises:

means for linking a first asset define to be in one asset type with a second asset defined to be in another asset type.

15. The system of claim 13, wherein the means for establishing the at least one relationship further comprises:

means for linking a first asset define to be in one asset type with a second asset defined to be in the same asset type.

16. The system of claim 13, wherein means (c) further comprises:

means for identifying one or more inventoried assets that relate to the identified criterion based on the at least one established relationship between the plurality of assets.

17. A system for assessing and/or managing risks for an organization, comprising:

a computer configured to identify a plurality of assets of the organization, wherein each asset is defined to be one of an electronic asset type and a location asset type, and wherein the electronic asset type includes computers and networking equipment therefor and the location asset type includes physical locations where the electronic asset types are placed;

a database configured to store the identified assets along with their asset types;

means for identifying at least one criterion defining a security objective of the organization, wherein the computer is further configured to identify one or more inventoried assets that relate to the identified criterion and configured to formulate one or more metric equations for each identified criterion, each metric equation being defined, in part, by the one or more identified assets, wherein each metric equation yields an outcome value when one or more measurements are made relating to the identified assets, thereby allowing a user to assess the risk to the organization based on the measured values of the one or more metric equations.

18. The system of claim 17, wherein the computer is further configured to:

electronically scan the plurality of assets;

interview members of the organization to identify the plurality of assets; and

manually identify the plurality of assets.

19. The system of claim 17, wherein the plurality of assets are defined to be one of a user type, a user population type, a data type and a network type in addition to the electronic type and the location type, wherein the user type relates to an individual user and the user population type relates to a group of users.

20. The system of claim 19, wherein the computer is further configured to establish at least one relationship between the plurality of assets.

21. The system of claim 20, wherein the computer is further configured to link a first asset define to be in one asset type with a second asset defined to be in another asset type.

22. The system of claim 20, wherein the computer is further configured to link a first asset define to be in one asset type with a second asset defined to be in the same asset type.

23. The system of claim 20, wherein the computer is further configured to identify one or more inventoried assets that relate to the identified criterion based on the at least one established relationship between the plurality of assets.

24. A computer readable medium including instructions being executed by one or more computers, the instructions instructing the one or more computers for assessing and/or managing risks for an organization, the instructions comprising implementation of the steps of:

(a) inventorying a plurality of assets of the organization, wherein each asset is defined to be one of an electronic asset type and a location asset type, and wherein the electronic asset type includes computers and networking equipment therefor and the location asset type includes physical locations where the electronic asset types are placed;

(b) identifying at least one criterion defining a security objective of the organization;

(c) identifying one or more inventoried assets that relate to the identified criterion; and

(d) formulating one or more metric equations for each identified criterion, each metric equation being defined, in part, by the one or more identified assets, wherein each metric equation yields an outcome value when one or more measurements are made relating to the identified assets, thereby allowing a user to assess the risk to the organization based on the measured values of the one or more metric equations.

25. The medium of claim 24, wherein the step (a) comprises the step of: identifying the plurality of assets and storing the identified assets into a database.

26. The medium of claim 25, wherein the step of identifying the plurality of assets comprises at least one of:

electronically scanning the plurality of assets;

interviewing members of the organization to identify the plurality of assets; and

manually identifying the plurality of assets.

27. The medium of claim 24, wherein the plurality of assets are defined to be one of a user type, a user population type, a data type and a network type in addition to the electronic type and the location type, wherein the user type relates to an individual user and the user population type relates to a group of users.

28. The medium of claim 27, further comprising the step of:

establishing at least one relationship between the plurality of assets.

29. The medium of claim 28, wherein the step of establishing the at least one relationship further comprises the step of:

linking a first asset define to be in one asset type with a second asset defined to be in another asset type.

30. The medium of claim 28, wherein the step of establishing the at least one relationship further comprises the step of:

linking a first asset define to be in one asset type with a second asset defined to be in the same asset type.

31. The medium of claim 28, wherein the step (c) further comprises the step of:

identifying one or more inventoried assets that relate to the identified criterion based on the at least one established relationship between the plurality of assets.